DATA PROTECTION POLICY

thinkproject

ISMS

Management system: ISMS
Product: ALL
Document ID: ISMS_00022
Version: 2.0
Classification: Open

Created by	Andreas Blücher	02.08.2022
Approved by	Tom Harman	02.08.2022
Date of original issue	03.08.2020	

Please do not print copies of this document.

CONTENT TABLE

Data Protection Policy
Management System: ISMS | Product: ALL
Document ID: ISMS_00022 | Version: 2.0 | Classification: Open
Created: 02.08.2022 | approved: 02.08.2022

1 PURPOSE

thinkproject is a collective of market-leading products and professionals with the goal to develop and deliver best-in-class solutions to support, connect, and advance the construction industry and the people in it.

This includes information and data processing on behalf of our customers. Therefore, customer information must be protected in terms of confidentiality and integrity. This Data Protection Policy describes how to achieve this goal and how to become compliant with legal requirements; especially the GDPR (General Data Protection Regulation).

Additionally, there might be contractually agreed obligations that have to be considered for example specific locations for data storage/processing.

The GDPR contains opening clauses to allow country specific regulation. To be compliant with national extensions of GDPR it would be pertinent to get advice from local consultants when implementing regional data protection policies.

2 AREA OF APPLICABILITY

The scope applies to the entire tp Holding GmbH group of companies that process personal data in the EU.

3 DEFINITIONS AND ABBREVIATIONS

3.1 Personal Data

In general, personal data is any information which relates to an identified or identifiable natural person. This could be for example:

- Name
- Postal address
- Email address
- IP-address
- Biometric data

3.2 Processing of Personal Data

In terms of GDPR processing of personal data means; any operation performed on personal data.

3.3 Lawfulness of processing

According to Article 6 of the GDPR; processing is lawful only when one of the below applies:

1. The data subject has given **consent**
2. Processing is necessary for the **performance of a contract**
3. Processing is necessary for compliance with **legal obligations**
4. Processing is necessary in order to protect the **vital interest of the data subject**
5. Processing is necessary for the performance of a task carried out **in the public interest**
6. Processing is necessary for the purposes of the **legitimate interests** pursued by the controller or by a third party

In most cases we will refer to 1, 2, 6 across our group of companies when considering the relation to our customers. In case of taxes or employment lax we will refer to 3.

3.4 Technical and organisational Measures

Technical and organisational measures are the functions, processes, controls, systems, policies, procedures and measures taken to protect and secure the personal information that an organisation processes.

3.5 Data Processing Agreement

A data processing agreement is a legally binding contract that states the rights and obligations of each party concerning the protection of personal data.

4 RESPONSIBILITIES

4.1 Data Protection Officer (terminology may vary country to country)

The conditions under which companies are obliged to appoint a data protection officer are regulated by national legislation. Companies are advised to seek advice on this issue from a lawyer specialising in data protection law.

The relevant Data Protection Officer (DPO) is responsible for being compliant with laws and regulations in terms of data processing. Their duties cover:

- Ensuring processes and products are compliant with GDPR and country specific regulations
- Maintaining local records of processing activities (Art. 30 GDPR)
- Interactions with data protection authorities
- Interactions with customers in questions of data protection

Small subsidiaries are permitted to hire external data protection officers after consultation with their Regional Manager.

4.2 Employee

Every employee may come into contact with our customer's personal data. **Every employee is therefore obliged to maintain the confidentiality and integrity of this data and to act compliantly with the law. To achieve this, employees must sign a data protection agreement (this can usually be found in an employment contract or an annex) and participate in data protection training.**

On the other hand, the employer processes personal data of employees. In the event of any questions concerning these processing operations, the employee shall contact the Data Protection Officer.

4.3 Information Security Officer

The Information Security Officer (ISO) monitors compliance with this policy. They support the Data Protection Officer in maintaining the confidentiality and integrity of the data.

The Information Security Officer and Data Protection Officer are both charged with ensuring confidentiality and integrity of personal data, and there may be times where the individuals facilitating these two roles will need to work together to achieve a mutually desired outcome.

Additionally, the Information Security Officer has to deal with availability. Measures to increase availability of data might influence the confidentiality of data in a negative way. In case of contradictions, DPO and ISO agree to achieve optimal protection of customer data and legal compliance.

4.4 Controller

With regards to client data our customers are the controllers when we process personal data on behalf of them.

With regards to employees or data collected in corporate websites we are the controllers of their data.

4.5 Processor

In terms of data protection, we are called the processor when we process personal data on behalf of our customers.

5 REQUIREMENTS

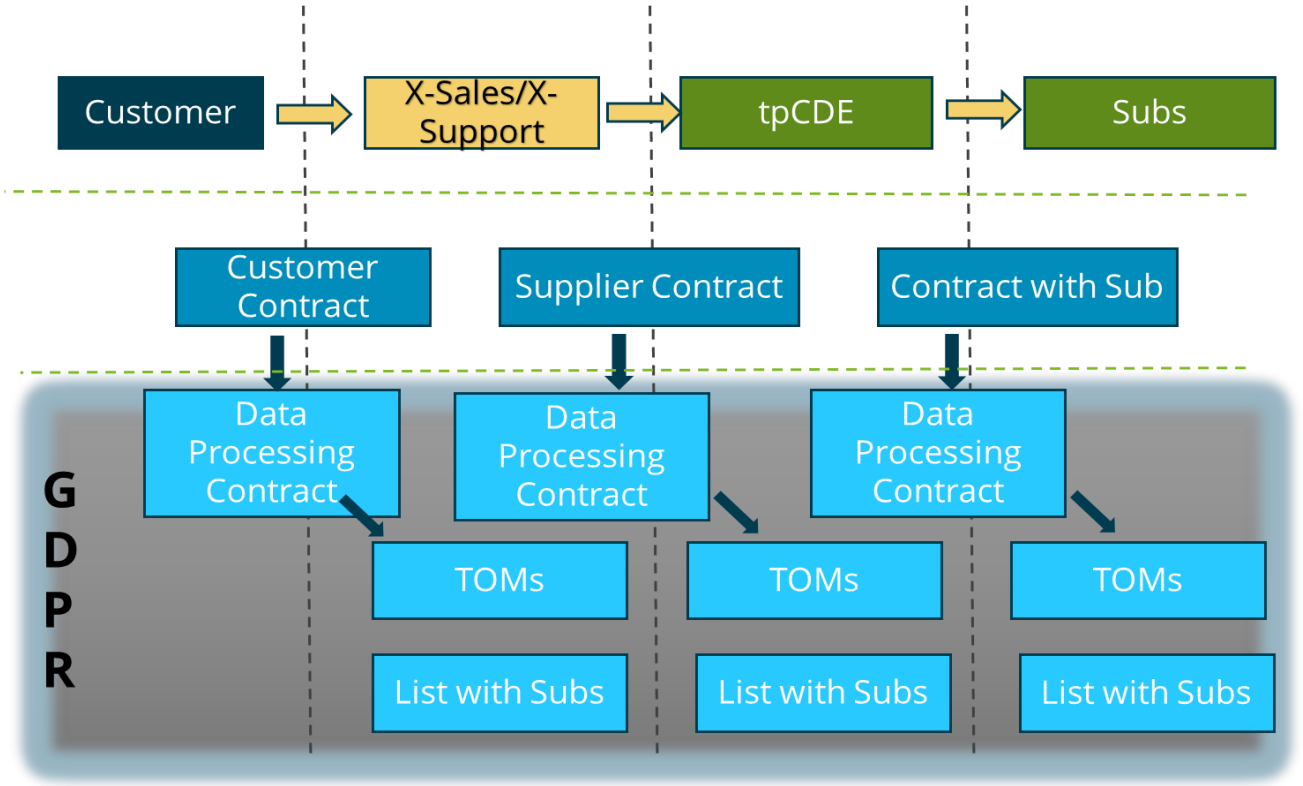
5.1 Principles relating to processing of personal data

Article 5 of the GDPR names six principles relating to processing of personal data:

- Lawfulness, fairness, and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality

5.2 Requirements of Data Protection in relation to our customers

When we process personal data on behalf of our customers, we must consider the following points:



The customer is usually at the beginning of a supply chain. They commission one of our sales offices to provide a service (for example a Common Desktop Environment (CDE)). The CDE service will be provided by one of the regional locations. To provide this service further subcontractors are engaged. When processing personal data within the CDE, GDPR requires the parties to sign a Data Processing Agreement (DPA) and to provide technical and organisational measure (TOMs) to ensure that the level of data protection remains consistent throughout the whole supply chain.

5.2.1 Data Processing Agreement (Article 28 GDPR)

Processing by a processor shall be governed by a contract. This contract is known as a Data Processing Agreement (DPA). This contract should state that the processor:

- processes the personal data only on documented instructions from the controller
- ensures that persons authorised to process the personal data have committed themselves to confidentiality, or are under an appropriate statutory obligation of confidentiality
- shall not engage another processor without prior specific or general written authorisation of the controller
- keeps the level of data protections at the same level even for new subcontractors

- provides technical and organisational measures (TOMs) to ensure data protection
- at the request of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes any remaining copies
- makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in the articles of GDPR, and allows for and contributes to audits, including inspections, conducted by the controller or another auditor mandated by the controller

Every location that provides software as a service and processes personal data of customers must provide a template for a data processing agreement. This template will be signed by both the processing thinkproject company and the customer.

This template of a data processing agreement must be approved by an internal or external consultant for data protection.

Sometimes sizeable customers provide their own template of a data processing agreement. This template must be reviewed by the data protection officer as a minimum and where necessary a lawyer to ensure compliance.

5.2.2 Technical and organisational measures

According to Article 32 of the GDPR the controller and processor of personal data must implement appropriate technical and organisational measures (TOMs) to ensure a level of security of personal data.

These TOMs include the description of measures to ensure:

- Access control (physical)
- Access control (logical)
- Separation control
- Relay control
- Entry control
- Availability control
- Control of Employees

Every location that provides software as a service and processes personal data of customers must provide a template of technical and organisational measures (TOMs). These TOMs become an annex to the data processing agreement.

TOMs must be reviewed by an internal/external consultant for data protection prior to being shared with any customers.

5.2.3 Subcontractors

If there is a need for further subcontractor(s) to provide a service to our customer(s) and these additional subcontractor(s) are going to process the personal data of our customers, it is required that the below are in place:

- A signed Data Processing Agreement with that subcontractor
- The subcontractor provides technical and organisational measures

5.2.4 Notifications of a data breach (Art. 33 GDPR)

In case of a data breach the controller (here the customer) shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority (for example the Information Commissioners Office (ICO) in the UK), unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

Therefore, if the data breach occurred within a part of the thinkproject group when processing customer's data, the customer (controller) must be informed at short notice to be able to act within the deadlines set. This is done by the relevant data protection officer. Every employee that observes a data breach immediately gets in contact with the data protection officer and opens an ISMS incident.

The period within which the customer must be notified is often subject of the data processing agreement (DPA) with the customer. It is fair to halve the 72 hours mentioned above in the DPA, i.e. 36 hours for the processor to notify the controller and 36 hours for the controller to notify the authority.

Additionally, it should be considered to consult a data protection lawyer in case of a data breach to minimize risks from litigations or fines imposed by the GDPR (Art. 83 GDPR).

5.2.5 Rights of the data subject

According to Chapter 3, GDPR the data subject has the following rights:

- Transparency and modalities
- Information and access to personal data
- Rectification and erasure
- Right to object and automated decision-making

Data subjects may ask the controller for their rights. In case that a thinkproject subsidiary is the controller of the data the rights must be pursued within one month.

In case that a thinkproject subsidiary is the processor, the controller (customer) must be involved. He is the contact person for the data subject.

5.2.6 Records of processing activities

Every type of processing activity that is executed as a processor must be kept in a record of processing activities log (Article 30, GDPR).

That record shall contain all the following information:

1. The name and contact details of the controller
2. The purpose of processing
3. A description of the categories of data subjects and categories of personal data
4. The categories of recipients of the personal data
5. Where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation
6. where possible, the envisaged time limits for erasure of the different categories of data
7. where possible, a general description of the technical and organisational security measures

The record is maintained by the data protection officer.

5.3 Requirements of data protection in software development

When developing software, product managers and software developers must consider the following points in 5.4 and 5.5.:

5.4 Product Managers

- Privacy by design (Article 25 GDPR)
- Privacy by default (Article 25 GDPR)
- Data minimisation
- Confidentiality and integrity of data
- Purpose limitation
- Storage limitation
- Implement functionality for the rights of data subjects

5.5 Software Developers

- Privacy by default (Article 25 GDPR)
- Data minimisation
- Confidentiality and integrity of data
- Storage limitation

6 EMPLOYEE AWARENESS

6.1 Thinkproject Academy

Every employee must complete the mandatory online training program "GDPR Awareness within Thinkproject" in the thinkproject Academy. In order to pass the course, employees must complete a quiz at the end of the course. When the questions are passed with a score higher than 85% the participant will obtain a Certificate which is accessible in the thinkproject Academy. The certificate is valid for one year, employees are notified shortly before the expiration of the certificate and requested to renew their certification.

Line Managers receive fortnightly reports by the Thinkproject Academy monitoring the attendance rate by their team. Line managers are responsible to ensure that their employees complete all mandatory trainings. Additionally, completion rates of employees are spot checked annually as part of the internal audits.

Currently the training is available only in English, however, this training will be made available in English, German and French starting Summer 2022.

6.2 Local Data protection policies

Local data protection policies required for that particular country's implementation of GDPR.

7 DOCUMENT CONTROL

Version	Date	Author	Approved by	Details of changes made
1.0	22.07.2020	AB	TH	Initial draft

1.2	28.07.2020	TH	AB	Review by TH
1.4	04.08.2020	Alan Brooks	Andreas Blücher	Review Alan
1.6	19.11.2020	AB	TH	Rights of data subjects
1.0	16.07.2021	KD	AB	New version numbering due to OneTrust import
2.0	21.11.2021	AB	TH	tpAcademy section with valid link and correct passing score
2.1	16.05.2022	KD	AB	Adjusting Section 6.1. (Removal of outdated link to academy environment, change of title section to awareness)
2.2	02.08.2022	AB	TH	Check for classification, set to open to be published on web site